EXHIBIT 6

Freedom to Tinker

… is your freedom to understand, discuss, repair, and modify the technological devices you own.

« MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug
CD Copy Protection: The Road to Spyware »

Not Just Another Buggy Program

Thursday December 8, 2005 by Ed Felten

Was anybody surprised at Tuesday's announcement that the MediaMax copy protection software on Sony CDs had a serious security flaw? I sure wasn't. The folks at iSEC Partners were clever to find the flaw, and the details they uncovered were interesting, but it was pretty predictable that a problem like this would turn up.

Security is all about risk management. If you're careful to avoid unnecessary risks, to manage the risks you must accept, and to have a recovery plan for when things go wrong, you can keep your security under control. If you plunge ahead, heedless of the risks, you'll be sorry.

If you're a parent, you'll surely remember the time your kid left an overfull glass of juice on the corner of a table and, after the inevitable spill, said, "It was an accident. It's not my fault." And so the kid had to learn why we don't set glasses at the very edges of tables, or balance paintbrushes on the top of the easel, or leave roller skates on the stairs. The accident won't happen every time, or even most of the time, but it will happen eventually.

If you're a software vendor, your software creates risks for its users, and you have a responsibility to your customers to help them manage those risks. You should help your customers make informed choices about when and how to use your software, and you should design your software to avoid exposing customers to unnecessary risks. Your customers expect this from you, and they'll hesitate to buy your product if they think you're leaving the cyberjuice on the corner of the table.

The design of the MediaMax/Sony software is a case study in risk creation. I wrote about these risks two weeks ago:

> But even if all [the software's spyware] problems are fixed, the MediaMax software will still erode security, for reasons stemming from the basic design of the software.
>
> For example, MediaMax requires administrator privileges in order to listen to a CD. You read that right: if you want to listen to a MediaMax CD, you must be logged in with enough privileges to manipulate any part of the system. The best practice is to log in to an ordinary (non-administrator) account, except when you need to do system maintenance. But with MediaMax, you must log in to a privileged account or you can't listen to your CD. This is unnecessary and dangerous.
>
> Some of the security risk of MediaMax comes from the fact that users are locked into the MediaMax music player application. The player app evades the measures designed to block access to the music; and of course the app can't play non-MediaMax discs, so the user will have to use multiple music players. Having this extra code on the system, and having to run it, increases security risk. (And don't tell me that music players don't have security bugs — we saw two serious security bugs in Sony music software last week.) Worse yet, if a security problem crops up in the MediaMax player app, the user can't just switch to another player app. More code, plus less choice, equals more security risk.

Sure enough, these risks enable the new attack, which exploits the presence of extra code on the system, and the fact that that code runs with full Administrator privileges.

The biggest risk of all, though, is that the software can install itself without the knowledge or consent of the user. When you decide to install a program on your computer, you take a security risk. But you take that risk knowingly, because

you have decided the benefit provided by that program outweighs the risk. If you change your mind about that tradeoff, you can always uninstall the program.

But if you decline the MediaMax licence agreement, and the software secretly installs itself anyway, you will face risks that you didn't choose. You won't even know that you're at risk. All of this, simply because you tried to listen to a compact disc.

Experience teaches that where there is one bug, there are probably others. That's doubly true where the basic design of the product is risky. I'd be surprised if there aren't more security bugs lurking in MediaMax.

Sony is still shipping CDs containing this dangerous software.

This entry was posted on Thursday December 8, 2005 at 8:01 am and is filed under Security, DRM, Privacy, CD Copy Protection. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

49 Responses to "Not Just Another Buggy Program"

1. *Greg* Says:
   December 8th, 2005 at 8:37 am

   I've been an avid follower of your posts and dissection of Sony's programming and consumer failure. For 36 days I've been battling with Sony Customer Service and their ContentProtectionHelp (ContentProtectionHelp@info.sel.sony.com) department working on this CD issue, with more than 14 e-mails back and forth and more than 3 hours logged on the phone.

   I want three things: -a "clean" version of the CD I purchased, -my computer 100 percent back to normal, -an apology and compensation for my trouble.

   To date, I haven't received any of these three, and Sony Customer Service has not offered any acknowledgement of error on their part. They appear to have lost my CD that I mailed back to them and blame me for that. They appear to have released a standalone uninstaller, but thanks to your insightful monitoring of their constant failure to release bug-free software, I do not trust them to run it. They have only offered me the option to wait until after 2006 when they will have a better handle on things.

   Considering I purchased/installed the CD/malware on Nov. 1, this is unacceptable to me as an unwitting consumer. But of course, they don't care. I'm just another dumb, complaining customer.

2. *Anonymous* Says:
   December 8th, 2005 at 8:43 am

   Ed, in your experience, what percent of software programs are completely bug free?

3. *Ed Felten* Says:
   December 8th, 2005 at 8:51 am

   Anonymous,

   All programs have bugs. The number and severity of those bugs, and the level of harm they inflict on users, varies greatly, depending on how responsible the vendor is about managing risks. Careless vendors make bug risks much worse.

4. *Anonymous* Says:
December 8th, 2005 at 8:55 am

So. like all other software, this software must have the bugs worked out. According to NGS, the problem in not uncommon and is easily fixed.

"After carefully researching the security vulnerability presented to us by SONY BMG, we have determined that it is not uncommon and, importantly, it is easily fixed by applying a software update."

5. *Ed Felten* Says:
December 8th, 2005 at 8:58 am

Anonymous,

Are you asserting that all programs are equally buggy? Or that it doesn't matter whether the vendor is careful? Or do you agree with me that the vendor's decisions affect the level of risk that users face?

6. *Anonymous* Says:
December 8th, 2005 at 9:09 am

What I am saying is that NGS, a security company, reviewed SunnComm's software and determined that the problem was not uncommon and is easily fixed.

As the problem is not uncommon, I am interested to know what experience has taught you regarding the responses from the other software companies you have dealt with on this same issue. I must admit that I have not followed your blog prior to this fiasco, but if you could reference some of the other programs you have found with similar problems I would appreciate it. Your exhaustive analysis and follow up may provide some much needed clarity to the situation. By providing a history of other analyzed software and the respective companies' responses, we would then be able to determine if SunnComm's response has been prompt or slow.

7. *Ed Felten* Says:
December 8th, 2005 at 9:10 am

By the way, the NGS quote isn't looking too good at this point. The patch that "easily fixed" the problem turned out to actually make it worse.

8. *Mike Birney* Says:
December 8th, 2005 at 10:00 am

""After carefully researching the security vulnerability presented to us by SONY BMG, we have determined that it is not uncommon and, importantly, it is easily fixed by applying a software update."

I think Anon is making 2 errors on the quote.

Because the security issue is NOT UNCOMMON is not an excuse to leave SunnComm off the hook. It may very well be an exposure that many programmers make when writing Windows code for the first time, or implementing some in-house software. But such a COMMON error like this should never get into a program that is going to be distributed to millions of customers, who don't have any inkling they are even installing software.

Just because it is COMMON for many investors to buy shares at the top of the market when even the bell boy is giving away tips and to sell at the bottom of the market when all is doom and gloom, is no excuse for a professional financial advisor to do the same. One pays professionals for their expertise in avoiding mistakes, not for falling into the pitfalls of amateurs.

The other problem with the SunnComm thinking (and I know you are one of the trolls, because I read Investorshub over the last few days and this is the argument that you people have been using to try and pretend

that what happened is normal in software development) is comparing MediaMax to Windows itself or to Oracle and then saying those programs have had errors too. But Windows XP and Oracle each involve hundreds of millions of lines of code, compared to Mediamax which doesn't have that much unique coding (much of it is just calls to Windows Media code supplied by Microsoft). A relatively small piece of unique code like MediaMax should be free of commonly encountered errors like this. Those errors should never have got by proper testing procedures.

Compare what Microsoft needs to test with Windows XP (and the multitude of combinations of everything) to what needs to be tested with Mediamax. There is no comparison.

Stop making excuses for incompetence.

9. *dr2chase* Says:
December 8th, 2005 at 10:01 am

I'm not Ed, but my estimate is "none", at least to an engineering approximation. This is why we play the risk-reduction game. And
there are bugs, and bugs — a stack buffer overflow is more risky than
a heap buffer overflow, because it is more likely to allow an attacker to
craft a worm. A break-in is a break-in, but a break-in to an account
with administrator privileges is worse.

Furthermore, in the presence of probabilistic algorithms (and there are many of these) or algorithms that contain counters that time out after a number of operations (2-to-the-64th nanoseconds is 580 years) a truthful person is forced to employ the weasel word "practically". In the asymptote, prime-factor-based security is not secure, and many counters overflow, so in some mathematical sense many working programs are actually "broken". Humans understand these dodges once they are explained, but they tend to complicate program proof, and they also force you to explore each person's definition of "practically".

10. *Anonymous* Says:
December 8th, 2005 at 10:02 am

Ed, NGS said it was a problem that could be fixed. It did not state that they looked at the patch.

How many other programs have you analyzed with this common problem and what was the response to your analysis?

11. *zapkitty* Says:
December 8th, 2005 at 10:14 am

You'll have to forgive the Sunncomm shill, Ed… twisting quotes wildly out of context is all they have left now. This particular Sunncomm shill spent the last day and night hammering that quote both here and over at the Investors Hub Sunncomm forum… aside from, that is, from saying that their "…software had Freedom To Tinker approval…" and that the "…EFF had agreed that Sunncomm had wrongfully been dragged into this by the XCP mess…"

Sunncomm's grabbing at any quote that can be twisted in any manner that can even remotely considered non-damning as their stock determinedly continues its valiant attempts to break the $.02 cents a share barrier and reach $.019… as SEC deadlines close in for various failures to file.

They are all out of options.

Sony's "DRM or Die!" campaign of deliberate malware infection is a nasty piece of work, but at least Sunncomm's antics do provide some graveside humor

12. *The PC Doctor* Says:

December 8th, 2005 at 10:21 am

More bad news for Sony/SunnComm

Geez, more bad news for Sony and SunnComm …
Today SunnComm released a patch for a security vulnerability in their MediaMax DRM software … problem is, the update suffers from the same security bug.
Question - are there any decent program…

13. *Jamie* Says:
December 8th, 2005 at 10:42 am

The Sunncomm shill is ignoring and masking the real issue by trying to concentrate on the bugs. The problem here is not whether the bugs are common in other programs or uncommon. The problem is that the user was NOT given a choice about installing the software. I use in my everyday work many programs that are known to have bugs. The difference here is that, I chose to install them and I can choose to uninstall them. So while the company that created those programs bears some responsibility for those bugs, I bear the majority of the responsibility for having the insecure software on my computer. In the case of the Sunncomm software I as the user, am not responsible in any way for my computer being insecure. Sunncomm made my computer insecure without my knowledge or consent. So they are completely responsible for all security issues resulting from their software.

14. *Dave* Says:
December 8th, 2005 at 11:19 am

Not to mention it's a program no one wanted or asked for when they thought they were buying a CD.

15. *Dennis D. McDonald* Says:
December 8th, 2005 at 11:26 am

Ed, I think the "risk perspective" is a very good thing to have introduced in this discussion. I agree: no software is ever "perfect." We make decisions based on a variety of factors about when it is appropriate to release new software, whether that software is intended for use by the public or by controlled populations within a corporation.

Clearly Sony did not understand the risks for liability it was getting into. The issue of its contract programmers' competence is related; Sony clearly did not understand enough about the (lack of a) testing process or about the variety of issues that would arise regarding the install/de-install processes surrounding both its DRM approaches. It seems to have missed the realization that its music division is now in the software business with all that entails.

Sony's problems have to do with both its attitude and with its ignorance about the market it is addressing.

Attitude-wise, Sony has a history of obfuscation about its DRM practices that I first uncovered last Spring when I was investigating whether or not the CD's I was buying online from various online vendors would actually play on my computer or on an iPod. I should have realized that something was amiss when the company I had been buying most of my CD's from over the past few years — BMG Music Services — basically refused to provide title-specific DRM information in its online catalog. While I published the result of my investigation in my blog ALL KIND FOOD I should have realized that the general lack of availability of title-specific DRM information from Sony was symptomatic of its attitude about its customers, an attitude that would eventually blow up in its face.

Regarding Sony's ignorance about the market it is serving: Sony's willingness to publish CD's that employ problematic (I'm being kind) approaches to DRM are leading it and its business partners to scramble to develop, institute, and support costly corrective processes and systems. I don't think it really knows what it's getting itself into by trying to "lock down" the use of products that retail for under $20. What portion of the sales price now has to go towards support for the labor and infrastructure costs for maintaining and supporting this worldwide

infrastructure of DRM it is instituting? How does this cost compare with what it hopes to gain from preventing piracy?

It's when I think about doing this type of cost-benefit calculation that I begin to believe that Sony's DRM is really not about preventing piracy, it's about competing with Apple — especially since it now appears to me that Sony, at least initially, was hiding the true extent of its DRM experiment.

- Dennis D. McDonald (http://ddmcd.squarespace.com/)

16. *tRellium* Says:
December 8th, 2005 at 3:03 pm

The problem is that I don't see suncomm learning from their mistakes and taking responsibility. I don't care for their current system of forcing their code into a computer, nad until they CLEARLY state they will not continue this behavior I simply don't ever want to see the Sunncomm name on any item in our house.

They come across as demanding of respect for their efforts, yet they don't particularly seem to have any respect for my computer and my demand that I control what software enters my system.

Its my computer, stay the hell out until I invite you in. Sheesh, maybe if I hang garlic from the CD tray it will keep the seemingly endless stream of DRM vampires away.

"Just say no to drugs and DRM", and life becomes clearer and simpler.

17. *Ned Ulbricht* Says:
December 8th, 2005 at 3:34 pm

Dennis,

Your belief that, "Clearly Sony did not understand the risks for liability it was getting into," has to be balanced against Bruce Schneier's November 17th, 2005 opinion in Wired that, "While Sony could be prosecuted under U.S. cybercrime law, no one thinks it will be."

A month ago, Eric Goldman, Marquette University Law School, wrote about XCP:

> Further, if the reports are true, the software's behavior could be a prima facie violation of the Computer Fraud & Abuse Act (18 USC 1030(a)(2)), which applies to an actor who:
>
> "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer…"
>
> Every computer connected to the Internet is a protected computer. The software allegedly obtains information (at minimum, the album being played). The phone-home "feature" may exceed the authorization given by the user; I don't think that mere consent to installing the software acts as consent to the reporting back of information.

Moreover, the Michaleson complaint has provided actual notice to Sony BMG about the provisions of the CFAA. They are not ignorant of the law.

If, as you allege, "Sony's DRM is really not about preventing piracy, it's about competing with Apple," then 18 U.S.C. § 1030(c)(2)(B)(i) "the offense was committed for purposes of commercial advantage […]"

Due to MediaMax, we now have an increased number of vulnerable machines on the network that may be used as platforms for attacks against my systems.

Further, my threat model needs to be updated if "reputable" corporations may now attempt to install software on my machines without authorization and with impunity.

BusinessWeek online reported on December 2nd, 2005:

> *[T]he complaints are being heard at the Justice Dept. "It's fair to say that we're aware of consumer concerns on the installation of this software on Sony products," says Justice spokesman Paul Bresson, though he declined comment on the number of Sony-related complaints the agency has received. "For now we're going to wait for more facts to become available and then evaluate what, if any, action is appropriate."*

I think we've waited long enough for a recall. At this point, this had better be in the hands of a Grand Jury.

18. *Dave* Says:
December 8th, 2005 at 3:37 pm

Like Dennis, I think the risk management angle is important here. Users that want to reduce "attack surfaces" in their PCs are careful about what they load and run. When software like SunnComm's installs–and runs!–despite the user's rejection of the EULA, they have increased the attack surfaces. If someone like Mark Russinovich is tricked into installing buggy Sony BMG CDs, what chance does an average consumer have?

All software has bugs, as the SunnComm trolls say. Most big companies that distribute software incorporate autoupdate features in their apps to ensure that unpatched bugs don't bite their customers. Sony BMG certainly qualifies as a big company, with millions of software installations at this point, but it has no software update infrastructure in place. If the XCP and SunnComm CDs continue to be sold and used–and they will be–the problem will get worse because many users won't realize the CDs have security issues. Each new system that is exposed to one of these CDs will be compromised. The solution is a recall. Then Sony BMG can go back and create the software infrastructure they need to distribute DRM.

19. *supercat* Says:
December 8th, 2005 at 8:28 pm

Actually, autoupdates can often create monstrous security holes by themselves (especially when controlled by malware producers). And must software doesn't need them because most software isn't buggy in a manner that would compromise security.

The bigger problem is that Sony's malware is designed to be non-removable. Thus, the normal method for dealing with security problems becomes impossible.

20. *Edward Kuns* Says:
December 8th, 2005 at 8:55 pm

The Suncomm trolls can be compared to someone who works for an auto manufacturer whose new model is highly prone to catastrophic failure (say, rollover or spontaneous fire or tire blowout) who try to mitigate blame by saying that ALL automobiles have problems when they are new. There is a profound inability to judge degrees of difference.

Yes, all software has bugs, but different categories of software need to be held to different standards for security. Software that is typically run without special priviledges does not require the same level of expertise to code as software that runs with special rights. User space software does not require the same expertise to code as kernel-space software. A bug in kernel-space software is often far more severe then a bug in user-space software.

And in this case, we have:

1) Software that is installed despite one refusing the EULA that
2) Users did not ask for and may not know is present that

3) Runs at kernel device-driver level to disrupt the CDROM drivers, and
4) Is small enough that it should be reasonably sure, and
5) Has no uninstall procedure, and
6) Until very recently required jumping through hoops to get an uninstall, but
7) The uninstall is buggy and security risk in its own right

That just does not compare to a bug in an operating system or a database server or a user-space application. Let's also take into account that while many vendors drag their heels on security problems, at least you know that the software is installed, how to uninstall it, who you bought it from, who wrote it, and where to find support.

21. *Dennsi D. McDonald* Says:
December 9th, 2005 at 5:17 am

Supercat makes a good point about auto-update features. I sort of trust the official Windows update processes (note the "sort of" qualifier) but I wonder about all the folks involved in the FireFox extensions and themes update processes, which I dearly love.

Ned's comments are a harsh note of reality — I'd prefer that Sony were punished in the marketplace rather than in the courts, just on principle, but maybe somebody does need to be taught a lesson.

I suspect, as others have mentioned, that the scope of the problem (regarding how many people have access to the innards of my computer that I don't know about) goes WAY beyond Sony and needs to be discussed more openly.

Dave's note that Sony needs to develop the infrastructure to support software maintenance and support again underscores all the expense that DRM users may be unknowingly committing themselves to.

22. *Dennis D. McDonald* Says:
December 9th, 2005 at 5:50 am

Ha! I mis-spelled my first name in the above post!

- Dennis McDonald (http://ddmcd.squarespace.com/)

23. *TomCS* Says:
December 9th, 2005 at 5:54 am

Ed

You are right that MediaMax discs need to be recalled, but not only because of the errors in its implementation. In the big picture, bugs and vulnerabilities are less important than the attempt to establish an unacceptable and excessively intrusive form of DRM, IANAL, but as far as I can see, the only legitimate objective of a software DRM scheme attached to audio discs is to limit the risk of purchasers abusing their "fair copying" rights, at least in those jurisdictions where that has been established.

From that point of view, both XCP and MediaMax are, to put it in other terms, hugely over specified: I cannot believe for example that phone-home/user on-line identification, or the installation of a new player application, is necessary to achieve the legitimate objective.

In practice, most reasonable music buyers could probably live with a DRM solution for CDs which mirrors Apple's burning and media/PC shifting restictions in the iTunes package for tracks bought from the iTunes shop. Is there any scope for the FOSS community to build a non-invasive alternative to XCP and MediaMax, and offer it to the record companies?

Clearly in present circumstances the business dynamic in the software DRM supply business is to set possible suppliers racing to produce the sneakiest and deepest and generally nastiest version they can: see for example the

many Sunncomm sales pitches and investor blurbs thrown up in this exercise. Even if the outcome of your and others' excellent work in exposing these attempts is to trash the two companies' reputations and even drive them out of this line of business, and kill these two packages as tenable options for the record companies, the dynamic will simply produce better built but equally over specified versions from other ambitious suppliers.

24. *Matt* Says:
December 9th, 2005 at 9:11 am

Sony owns thier own DRM company with Phillips called Intertrust so Why are they bothering with Sunncom and First4Internet.

www.intertrust.com

25. *Anonymous* Says:
December 9th, 2005 at 9:59 am

UPDATE (Dec. 9): Sony and MediaMax have issued a new patch. According to our limited testing, this patch does not suffer from the security problem described above. They have also issued a new uninstaller, which we are still testing. We'll update this entry again when we have more results on the uninstaller.

http://www.freedom-to-tinker.com

26. *josh* Says:
December 9th, 2005 at 10:57 am

–
The best practice is to log in to an ordinary (non-administrator) account, except when you need to do system maintenance. But with MediaMax, you must log in to a privileged account or you can't listen to your CD. This is unnecessary and dangerous.
–

This is entirely untrue, yet you keep repeating it. Once MediaMax is installed, you do not need to run as administrator. Any security risk is a different issue, but the security risk of needing to run as administrator is untrue.

The only reason there is ANY issue at all is because the software installs some components without accepting the EULA.

Once that one issue is solved, this whole sensationalist fiasco falls apart. Every other week Internet Explorer has a security issue that is just as severe. The only reason Microsoft isn't torn apart over this is you have to accept the EULA first.

Again I ask where is the analysis of Macrovision's products? Why are you bent on MediaMax? You didn't even look at XCP; it took others to find it. XCP blew up all by itself and you take that, spin the mob mentality that it's stirred up and try to tie it to MediaMax.

Does anybody else not see an agenda here? If you hate DRM, at least hate it equally.

27. *Ed Felten* Says:
December 9th, 2005 at 11:18 am

Josh,

The only way to resolve the install-without-EULA problem is to recall the discs with that "feature". Or do you advocate leaving millions of infected discs out there in the marketplace?

And while making a secure browser is really hard, making a secure compact disc is easy — even tiny record labels have been doing it for years. All you have to do is avoid putting software on the disc.

Similarly, it's very easy to avoid installing software without permission. All you have to do is make sure you get permission before you install any files or put anything into the registry.

28. *Anonymous* Says:
December 9th, 2005 at 11:20 am

"It's a fairly common issue often found in PC games," said Robert Horton, a security expert from NGS Software brought in by Sony to vet its latest patch.

"Its fairly common and the fix is easy to provide through a software update."

He said it was unlikely that any attacker would have been able to exploit the bugs in MediaMax and its patch.

29. *Jesse Weinstein* Says:
December 9th, 2005 at 1:24 pm

Are the SunComm shrills using a bot to post, now? The message above, from "Anonymous"(why are they so afraid to identify themselves?), is an exact repeat of various other messages. Stop shooting, folks, you're just aiming at your own feet.

josh - You claim: "Once MediaMax is installed, you do not need to run as administrator." This is not the actual claim, or point. The point is that the MediaMax *runs* with administrator access. Otherwise it could not alter the operation of the CD drive, which is it's intended purpose. This has been explained numerous times. If you dispute that claim(that MediaMax runs with administrator access), please provide some evidence or sources to back this up.

Otherwise, this just looks like more spin, and intentional misunderstanding.

30. *Josh* Says:
December 9th, 2005 at 3:39 pm

—
The only way to resolve the install-without-EULA problem is to recall the discs with that "feature". Or do you advocate leaving millions of infected discs out there in the marketplace?
—

The only portion that runs with administrator access is the kernel component that interferes with the operation of the CD drive. All other components (user interface, player, etc) run as the logged in user.

An easy way to demonstrate this is to take a MM-5 CD, install it (as administrator), then once installed log in as a normal user and run the SecureBurn feature. Without a program like nero burn rights, only an adminstrator can perform write operations on a CD drive under Windows 2K/XP.

AFAIK the kernel component has yet to be exploited, which makes any exploits found non 'root' exploits, as if the attacker would gain elevated privledges. Access to the system and elevated privledges are not the same thing, but I digress. The difference doesn't matter much under Windows.

You are right about the issues though. All drivers run in kernel mode, so any DRM system that relies on a driver to function has a potential security risk, by design.

—-
And while making a secure browser is really hard, making a secure compact disc is easy — even tiny record labels have been doing it for years. All you have to do is avoid putting software on the disc.

To the copyright holder, the compact disc is anything but secure. There are two sides to copyright and your 'solution' only looks at one side. Ask any software company that's put a 'cd key' on their CDs. It's Ok for software to be protected by a 'cd-key' but it's not ok for music?

If only all intellectual property owners would trust your solution then maybe I could use my 'fair-use' rights and install Windows without the CD key I lost. Also, I wouldn't need to send various pieces of private information to a server somewhere in order to 'authenticate' my new install of Windows.

By requiring a CD key, Microsoft is assuming you are a thief, yet everyone understands its purpose and accepts it without feeling violated. You apply the same concept to a music CD and people feel like their rights are being violated.

31. *Anonymous* Says:
December 9th, 2005 at 4:05 pm

MediaMax CEO, Kevin Clement, Comments on Recent Events

"I am incredibly excited to be here at MediaMax Technology. MediaMax and SunnComm are two fantastic organizations defined by talented and dedicated team members. These organizations have consistently delivered solid, tested and certified technology solutions for years," comments Kevin Clement, MediaMax's recently appointed and on-the-job president and CEO. "I intend to develop a world-class technology organization focused on delivering high-quality, secure, consumer friendly content protection solutions.

I have been working closely with our record label customers, security firms and other industry groups to ensure that we are addressing any and all concerns regarding our industry-leading MediaMax product. Recently, our software has come under intense scrutiny from the technical community following a series of accusations relating to security issues and code infringement against one of our competitor's products. We take all potential security issues very seriously. As such, our teams respond immediately upon notification of any potential security vulnerability."

SunnComm is a software company. Software companies routinely issue patches and updates. This is not uncommon and is an accepted practice. Due to the structure of current operating systems, we all are constantly reminded of the need to upgrade software for various reasons. This process applies to software that we use every day including media players, browsers, word processors and even the operating systems themselves. The reality is that we will be called upon from time to time to issue patches and updates to our software. We understand and accept this responsibility. We always strive to deliver well designed code that is 100% bug free and provides secure solutions. As history has shown, this is not always possible to do, even for the largest software companies.

The true worth of a software company is not how perfect their code is, it can never be perfect, but rather how quickly they respond to valid concerns regarding the security and stability of their product and more importantly, how quickly and efficiently they deliver a solution. MediaMax Technology takes potential security vulnerabilities very seriously. This will never change. Recent news events along with an increased level of scrutiny have created challenges for our entire industry. MediaMax Technology, along with our strategic partner, SunnComm International, has responded quickly and with decisiveness. SunnComm has consistently worked with its partners and multiple software security firms in order to thoroughly test and ultimately deliver completed secure resolutions. We have delivered these in a timeframe of days where the norm in the software industry is to respond within a month. We will always strive to deliver corrective solutions in a period of time that exceeds the expectations of our customers and their consumers.

There are very vocal groups and individuals who do not believe in the use of DRM technology. This is a philosophical debate that will not be settled anytime soon. MediaMax Technology's responsibility is to deliver content protection solutions that balance protecting the intellectual property owner's rights and the expectations of their consumers. We are focused on delivering high-quality, secure, consumer friendly content protection solutions.

Kevin concludes, "Our software solutions are being improved every day. You have my word that we will not stop working to make our products better, more secure, more consumer friendly and more valuable to our customers. As we emerge from this period of intense scrutiny, our solutions and, more importantly, our company will be better because of it. I would like to point out that no other CD or DVD copy protection technology has ever undergone the type of intense scrutiny that MediaMax has encountered. The development team has addressed every valid issue that has been presented and has made the necessary adjustments. The current MediaMax product is now the most secure, tested and scrutinized copy protection technology available anywhere in the world. We intend to immediately begin leveraging this incredibly stable, well-tested core technology in our plans to develop and deploy new content protection solutions in new markets and industries. Our mission is clear - develop a world-class technology organization focused on delivering high-quality, secure, consumer-friendly content protection solutions. These recent events have served to make us battle tested and better then ever."

32. *Anonymous* Says:
December 9th, 2005 at 10:53 pm

Ed, this statement should be officially retracted along with a letter of apology…

"Was anybody surprised at Tuesday's announcement that the MediaMax copy protection software on Sony CDs had a serious security flaw?"

According to the security experts…

"It's a fairly common issue often found in PC games," said Robert Horton, a security expert from NGS Software brought in by Sony to vet its latest patch.

"Its fairly common and the fix is easy to provide through a software update."

He said it was unlikely that any attacker would have been able to exploit the bugs in MediaMax and its patch. "

Just because you obviously have little experience with this type of software flaw, does not entitle you to use these inflammatory statements. (If you do have experience with these common issues that are easily fixed, then why are you characterizing them in a different light?) According to the experts, there never was a 'serious security flaw' with this issue.

Additionally, your comment…
"By the way, the NGS quote isn't looking too good at this point. The patch that "easily fixed" the problem turned out to actually make it worse. "
…should also be retracted. The fact is that your continued criticism of the common and easily fixable problem is what isn't looking too good at this point.
I anxiously await your retractions, corrections and apologies.

33. *Edward Kuns* Says:
December 10th, 2005 at 12:09 am

Josh — What planet do you live on where you believe "By requiring a CD key, Microsoft is assuming you are a thief, yet everyone understands its purpose and accepts it without feeling violated."? Ask those people who are directly accused of being a thief for making the "error" of changing too many hardware parts and getting the third degree from Microsoft before being allowed to use the computer and OS they legally bought. Ask the folks who started finding non-Microsoft solutions because of their displeasure with the activation model.

And that's activation. A CD Key does not assume you are a thief. It is closer to a key to start a car. It keeps honest people honest but does not deter the serious thief. The difference is that a key does not impede one's ability to use a car. A CD key usually does not impede one's ability to use the software (unless you lose it and have to reinstall). Activation very well might prevent you from using the software you legally bought. And here is the kicker — CD keys and activation do not deter the determined hacker. Not at all. Not even a little bit.

The same can be said for DRM. These are systems that prevent the honest from making legal use of what they have legally paid for, but that do not truly prevent illegal use. This leads me to conclude that piracy is not what DRM is about, because no DRM scheme out there today does much of anything to prevent piracy.

And to anonymous who is awaiting Ed's retractions, etc, wow! OK, I know, don't feed the troll and all, but one should not hold DRM to the same low standard that game software is held to. It's like having an airline fall out of the sky and having someone say, "Yes, it was a mechanical problem. But it's a very common mechanical problem. This problem occurs on lawnmower engines all the time."

That an issue is "common" is NOT an excuse. OK, DRM will not take anyone's life, but for Sony/BMG to secretly have software installed on people's computers and then to find out that that software has "common" errors, that just rubs salt in the wound. It means that their programmers were unskilled. It makes one wonder — if there are *common* errors in that code, what other errors will be there that haven't been found yet?

Also, remember that game software is far more complex than MediaMax.

34. *Josh* Says:
December 10th, 2005 at 2:10 am

—
The same can be said for DRM. These are systems that prevent the honest from making legal use of what they have legally paid for, but that do not truly prevent illegal use. This leads me to conclude that piracy is not what DRM is about, because no DRM scheme out there today does much of anything to prevent piracy.
—

By your logic then, CD-keys are not about piracy because they do nothing to prevent it? What are CD-key's purpose then? This I want to here.

DRM is about piracy. CD-keys are about piracy. It does not have to stop 100% of piracy to be effective. If it costs $10,000 to make copy protection software (even a CD-key system) that only stops 1% of piracy in a multi-million dollar market, it's still worth it to the content producer. What other reason does the CD key exist for?

–
A CD Key does not assume you are a thief. It is closer to a key to start a car. It keeps honest people honest …
–

So you admit in your own argument that a CD-key does in fact have some effect; it keeps honest people honest? You mean it keeps people that don't have the technical know-how to download a key-gen to pirate so they give in and buy instead?

The concept of lock and key in itself assumes theft. If there were no thieves you wouldn't need to lock your doors. You wouldn't need locks or keys at all. To use your analogy in this context is illogical.

By your analogy a naked audio CD is an automobile with a push-button ignition and no locks on the doors.

Adding a limiter to the speed of your car so that it cannot go about 100mph doesn't take away your 'right' to drive, but it does impede the usage of your car. Most people would accept this because it's only when it's illegal usage.

DRM impedes your usage, but it should only impede usage that would be deemed illegal.

–
That an issue is "common" is NOT an excuse. OK, DRM will not take anyone's life, but for Sony/BMG to secretly have software installed on people's computers and then to find out that that software has "common" errors, that just rubs salt in the wound. It means that their programmers were unskilled. It makes one wonder — if there are *common* errors in that code, what other errors will be there that haven't been found yet?

Maybe their programmers knew full well of the security issues involved, told management, and it fell upon deaf ears?

Not that I would know.

35. *Edward Kuns* Says:
December 10th, 2005 at 8:27 am

Josh, you are correct; my analogy was flawed. I'll try again.

First of all, I believe that few consumers would complain about DRM that *only* prevented ILLEGAL use. A CD key, an auto key, a house key fit this model, except to the degree that one loses the key and is locked out of what you own. Consumers accept these keys because they are non-invasive, simple, and without other side affects. Consumers accept the responsibility of needing to keep the key, because it is simple and non-invasive. This is what I meant by "keeping honest people honest."

The DRM in question here actively impedes many legal uses, such as copying the music to an iPod. In addition, the license agreement is offensive in its terms.

Locks discourage casual theft, joyriding, but do not discourage a determined thief. Auto locks and home locks exist for other important reasons as well — to keep unwanted people out of your home. Someone don't have to steal stuff to be unwanted. An unlocked house would allow entry to every salesperson, religious advocate, political advocate, and passerby.

Here is another point: Home and auto locks protect the OWNER, not the manufacturer or distributer. Consumers are not legally required to use keys and locks, and if they choose to remove the locks, no law will stop them. A person who is physically incapable of using the locks as provided can remove them totally or replace them with something their special needs require.

A co-worker of mine is in a wheelchair. His auto is modified to use hand controls. This is possible because the auto manufacturer does not *require* you to use their controls. Thus, the manufacturer does not have to build for all possible abilities and disabilities. They can rely on the aftermarket to handle special cases. The DRM in question here does not fit this model. If you cannot use their player/copier then you are out in the cold. Unless you get someone else to go through the software to make a copy they can use on a computer.

Here again is a key point (pun not intended): I believe that consumers will accept a non-invasive DRM that does not impede legal use. A DRM that runs in kernel mode and that interfers with the proper operation of a computer is invasive. A DRM that phones home before you can use your computer (WinXP) is invasive.

Let's talk costs. These DRM schemes are not cheap to create. In the US, a cheap inexperienced software developer can be had for maybe $30k a year. Let's say you have a small team of 5. That's $150k a year. (This doesn't include the cost of benefits.) Give then a manager at $50k a year. That's $200k a year. Assuming they develop everything from scratch for one operating system, it would maybe take a year or two to produce. We've now spent between $200 and $400k in wages alone, not including hardware costs, sales, HR, IT, documentation, senior management, electricity, rent, and so on. And that's for inexperienced developers. We're talking low millions to develop a DRM scheme, minimum.

All of this convinces me that DRM is more about market control and vendor lock-in than it is about piracy.

36. *tRellium* Says:
December 10th, 2005 at 1:32 pm

Dennis McDonald wrote:

Ned's comments are a harsh note of reality — I'd prefer that Sony were punished in the marketplace rather than in the courts, just on principle, but maybe somebody does need to be taught a lesson.

_____

I agree with most of what you said, but I don't feel much simpathy for Sony regarding having to defend themselves in a court of law. Looking at summaries such as the one at EFF's history archive:

http://www.eff.org/IP/DMCA/?f=unintended_consequences.html

shows that Sony is more than willing to use the courts in an aggressive manner, so why should they be exempt from defensive lawsuits themselves?

37. *Dennis D. McDonald* Says:
December 11th, 2005 at 11:39 am

tRellium: please do not assume that I have "sympathy" for Sony. I just prefer the marketplace solution over the legal solution. Just because Sony is willing to use aggressive legal tactics doesn't mean I condone such tactics.

On the other hand, I do have sympathy for Sony employees who have to "clean up" after the mess their bosses made with their DRM implementatons. I've already addressed this in an earlier entry from my own blog: "But my heart does go out to "John" and all the other Sony BMG staff members, administrators, clerks, customer service reps, technicians, secretaries, warehouse workers, and everyone else who will have to pick up the pieces for this astoundingly wrongheaded exercise in anti-customer behavior." (from http://ddmcd.squarespace.com/managing-technology/sony-responds-to-my-santana-inquiry.html)

38. *Ned Ulbricht* Says:
December 11th, 2005 at 3:08 pm

Dennis,

I would daresay that I have a certain amount of sympathy for the Sony organization. When I think of Sony, I think first of Sony v Universal City Studios and second of the Sony Walkman. There is a reason why Sony has been consistently considered one of the most reputable corporate brands.

But in an orderly society, there exists no more corrosive influence than the appearance that some people or groups are above the law.

39. *Bruce Hayden* Says:
December 12th, 2005 at 2:02 pm

The Media Max prospectus referenced in another thread makes interesting reading. It appears that much of the Media Max / SunnComm DRM code problems are intentional. They appear to have intentionally hidden the code and to have intentionally snuck it onto computers. These are considered pluses in the prospectus.

40. *Bruce Hayden* Says:
December 12th, 2005 at 2:11 pm

My personal belief is that Sony, Media Max, et al. lost track of the equities here. In that Media Max prospectus I mentioned above, they claim:

> "The latest data available from the MPAA estimates that the U.S. motion picture industry lost in excess of $3.5 billion in 2003 due to packaged media piracy. Music industry unit ("CD") sales have been falling approximately 10% year-over-year for the past four years, according to the International Federation of Phonographic Industries ("IFPI"). In addition, the International Intellectual Property Alliance ("IIPA") estimated that copyright piracy, not including Internet piracy, around the world

inflicts $20-$22 billion in annual losses to the U.S. copyright industries."

If the market shares are equal for the big 5 record companies, etc., then this translates into $700 million lost to packaged media piracy, and $ 4 billion or so in copyright piracy, not including Internet piracy. Even if you can't get Sony's share by dividing by 5, you can get an idea of the magnitude of the company's problems. It sees hundreds of millions, if not billions of dollars a year in lost revenue due to piracy. And, as a result, probably felt justified in utilizing all these intrusive DRM systems.

41. *supercat* Says:
December 12th, 2005 at 5:40 pm

Record companies inflate their "losses" by assuming that every copied track represents a lost CD sale. So if a kid with $10/week to spend downloads 10 songs per week, the music company figures that as over $100 loss notwithstanding the fact that the kid couldn't have possibly spent $100/week on music even if we wanted to.

For that matter, if someone downloads a track, decides he likes it, and then goes out and buys the CD, the music company still considers that a "loss".

The record company figures I've read claim that half the music out there is pirated. Even if that is true, that represents nowhere near a 50% loss of revenue. If record companies were really interested in revenue, rather than control, they would work more to encourage downloaders to become paying customers, rather than regarding them as enemies.

42. *tRellium* Says:
December 12th, 2005 at 8:01 pm

Hmmm, $22 billion dollars lost to piracy of a $10 CD? Thats 2 billion CDs per year. Can they even produce that many? Who would listen to all that?

Have they ever sold that many records in one year, let alone CD's? They never considered that someone downloaded a copy and then bought a CD or purchased the songs from iTunes, or never listened to it again?

If I hear a song on the radio and don't like it enough to buy a copy, it obviously shouldn't rate as a lost sale to SonyBMG.

Sounds like a pie-in-the-sky estimate of losses, but then again they are driving only the honest customers away with these DRM systems. The pirates and illegal downloaders aren't even slightly impacted by these issues. Only the honest/unsuspecting are impacted.

Many of the artists listed on the SonyBMG webpage for product alerts have their music downloadable at iTunes. Several of them are really very good too, I have added 3 of them to my shopping cart but I won't be getting the CD's.

If SonyBMG wants to list that as a "lost sale", that's just fine with me.

43. *Bruce Hayden* Says:
December 14th, 2005 at 8:40 am

The $22 billion claim really doesn't make sense, does it?

My view is that Sony does feel under seige here, and took the law into its own hands, essentially crossing the line into illegality, or, at a minimum, violated any number of consumer protection laws. I at least get this feeling reading the stuff from Sony / Media Max / SunnComm trolls, that they felt justified based on their perception that they were losing huge amounts of money through piracy.

Which I think is one reason that they shipped this stuff full of bugs. They believed they were the ones wearing

the white hats and riding to the rescue.

But I think that this led them to not think this whole thing through, including the important fact that the software would ultimately be installed on millions of computers. And any software that is going to be that widely installed, should be much closer to bug free than what we saw here. Much closer.

I am running an email server with market penetration in probably the dozens. I expect bugs, and, see them once in awhile. But the project is small enough that that is not an issue. On the other hand, you have MSFT, with market penetration in the hundreds of millions. Bugs there also exist, but are much less common because the company has learned over time that it is cheaper and better in the long run to get rid of most of the bugs before shipping the software. But that, of course, means a lot of expensive testing, etc. Also, sometimes product ship dates are missed. Used to be with MSFT, they would ship a product mostly on time even if buggy. Now they are driving their releases much more by product stability than they used to. (And I know they aren't perfect - just improved).

Which brings us to Sony. They should have required their contractors to test closer to the MSFT level, given that they would be installing on millions of computers. But the level of test seems more akin to that of the email server I run. They never thought through that buggy software + millions of installs = major problems. And, then, under the heat of publicity about their bugs, they rushed patches out that may have made things worse.

44. *Scott* Says:
December 14th, 2005 at 3:50 pm

Edward Kuns:
"Also, remember that game software is far more complex than MediaMax"

wow, so how many games have you written anyway? or for that matter, copy management software? a bit grandiose and general, wouldn't you say?

tell ya what, try an experiment for me. design a fool-proof, non-intrusive way to stop (or at least diminish) audio cd piracy, that gives everyone their rights and performs to everyone's expectations of what they think the software should be.

ok, now here's the clever bit: wait for it… wait for it… totally bug free.

you have absolutely no idea how many lines of code there are, nor the complexity of taking raw audio, streaming it, and encoding it.

let me clear up a few things for you good folks. the shift key thing? was, and is *not*, a 'trick' or 'discovery' or 'workaround' or 'hack' or anything else Mr. Felton or Mr. Halderman would have you believe. any idiot that has ever put together anything resembling a cd, will tell you that the autorun feature can, and will most likely be 'side-stepped' by the shift key and has been around since way back in the day. the developers knew this from day one. it was never hidden from anyone, it was and *is* common knowledge of the operating system.

secondly, and i stress this: THERE IS NO SPYWARE IN MEDIAMAX!.. not in any version! it simply tries to connect and download a jpg to display with an html link to an artists site. if it can't connect, it simply shows a static image.

thirdly, just as developers don't run the company, nor do they influence it's politics or the politics of the industry as a whole. if Apple wishes to 'turn on the switch' so-to-speak, then fine great, MediaMax is already enabled to do it.

fourthly, the term 'infected' is decidedly antagonistic. what was infected? how does the software stop you from listening to the music? or making copies? or even encoding them to your harddrive to listen in mediaplayer? or in your car stereo? or an SDMI compliant device? even *if* IPOD support is null right now, does *not* mean that it won't ever be able to support it. if they simply 'turn it on', all of those MediaMax discs will now enable you to

export to IPOD.

as i see it, if anything, it simply stops you from doing something you probably shouldn't have been doing in the first place, otherwise, what does it stop you from doing?

btw, when did this become an alternate home for the investor hub people, as a way to incite riot amongst folks who might not know better?

btw, to anyone that has downloaded stuff off of p2p illegally. whether or not you realize it, real folks are being hurt when you do it. get enough people doing it, and people start losing their income, and i'm not talking about the music companies. i'm talking about print shops, t-shirt shops, writers, sound engineers, delivery people, store clerks etc etc. they all, in some way, make their living off of cd's and the music on them.

so while everyone here is waxing poetic about this right and that right, in the meantime, if nothing is done, there are real folks getting crapped on..

keep that in mind..

45. *supercat* Says:
December 17th, 2005 at 10:06 am

THERE IS NO SPYWARE IN MEDIAMAX!

It walks like a duck, smells like a duck, and quacks like a duck, so it must be a giraffe, right?

Spyware is software that installs covertly on a machine without the owner's informed consent, tries to make itself difficult to remove (or in some cases even detect), and monitors what the user does with the system so it can act when the user does something it finds "interesting". Mediamax installs itself without the system owner's informed consent (walks like duck), tries to make itself hard to uninstall (smells like duck), and watches for anything that looks like CD drive access by unapproved applications so it can break it (quacks like duck).

46. *Edward Kuns* Says:
December 18th, 2005 at 10:24 pm

OK, Scott, let me say that there are no personal attacks intended by my saying that game software is more complicated that MadiaMax or XCP. Simply looking at the size of the applications in question gives a relative measure of complexity. The smaller the binary file, the more surprising it is when bugs are found. (Assuming code written by equal quality software folks.) Also, the closer code is to the operating system, the more outrageous it is when bugs and security problems are found.

I have written neither commercial games nor commercial DRM. However, I have worked on a real-time data acquisition system for a high energy physics experiment, an operating system for a telephone switch, firmware for components of a telephone switch, audio drivers for a RTOS, and numerous other projects involving a few to hundreds of developers and a very high requirement for reliability. I have known people who wrote commercial games. I have never known anyone who wrote commercial DRM or even non-commercial DRM.

Grandiose and general? No. It's a simple and reasonable observation given the relative side of the binaries. Yes, OS drivers require more care than something written outside the OS. But not only do games stream audio, mixing audio from multiple sources, they also display real-time video, maintain state information, perhaps maintain state of many other players in the game, and manage a large quantity of information. And a game is software someone deliberately installed.

Scott, if the shift-key thing was such a non-issue, why did the company threaten to sue over someone revealing it?

Also, do you understand why software that secretly installs itself, is deliberately difficult to remove, and that

pings a server to pull down images or whatever can be considered spyware? You do understand also that many SPAM messages include image links that if loaded allow the SPAM senders to know the EMail address is valid? All of this leads people to call MediaMax spyware. This is opposed to software that one knowingly installs, that one can safely and easily uninstall, and that performs a function the user wishes.

The term infected? That term is appropriate for anything that installs itself secretly and that is deliberately difficult to remove. This is even more true for anything that interferes with the normal functioning of one's computer.

If Apples does not license its DRM, then how can MediaMax be already ready to interoperate with it?

And here is some news that has been stated here many times. Let me say it again. For a red-book audio CD or anything that will play such audio CDs, THERE IS NO EFFECTIVE COPY PREVENTION.

Finally, I have not downloaded or shared music. Never. Not once. All of my use of any filesharing network has been entirely legal — downloading only that which is deliberately shared. Namely Linux software distributions. I don't know if you are making this assumption or not, but many of those supporting MediaMax or XCP seem to assume that anyone who is against DRM (as implemented today) is *for* open sharing of all music and video. If there were an open-standard non-intrusive non-invasive DRM that allowed fair-use rights while protecting the artist rights as well, most people here would support it, I believe. It is probably impossible for audio CDs to ever support such DRM however, given the nature of the standard.

47. *Edward Kuns* Says:
December 18th, 2005 at 10:28 pm

Let me correct myself. A little over a decade ago, I did help in porting a commercial game from a BASIC environment (obviously the game was not written in basic but was just written to execute in that environment) to a RTOS. I did maybe 5% of the porting work, maybe less. But I have never written nor worked with anything approaching DRM.

I don't have to have written DRM to be able to estimate the level of complexity however.

48. *Sony BMG Issues New Security Patch for Audio CD Software Problem - Tech Trends - NewsFactor Network* Says:
January 9th, 2006 at 9:15 am

[…] "However, we do agree with the position taken today in Ed Felten's blog - 'Experience teaches that where there is one bug, there are probably others.' That's doubly true where the basic design of the product is risky. I'd be surprised if there aren't more security bugs lurking in MediaMax." […]

Leave a Reply

Name

Mail (will not be published)

Website

Submit Comment

Powered by WordPress.
Entries (RSS) | Comments (RSS).